



There has been a lot of emphasis lately on computer security and the menace of cyber warfare. However, having surveyed the field and sifted through all the things that can go awry from an information security standpoint, I have come to the following conclusion: *We are the weakest link.*

And by “we” I mean, of course, all of us who form the sentient carbon-based portion of our IT systems. Yes, worms, viruses, bot-nets and other means of attack are legitimate threats. However, even these technology-based bad actors generally take advantage of human nature to inflict the most harm to our systems.

Information technology and business journals abound with stories of security breaches caused by careless, ignorant or optimistic users fooled by clever hackers. Reports on hardware compromises frequently mention that hackers used social engineering to extract key information from employees that helped them crack systems.

The “script kiddies” who download automated tools and use them to crack systems through purely technical means are at the low end of the hacker scale. As Bruce Schneier, my favorite security guru, observed, “Amateurs hack systems, professionals hack people.”

For an example of a real pro, I offer Kevin Mitnick, arguably the most notorious hacker of modern times, who relied heavily on human vulnerabilities to get into the computer and phone systems of American government agencies, telecommunications carriers and technology companies. While he also used attacks like IP spoofing, he gained most of his illicit access simply by conning people. We will discuss why cons are successful later.

Therefore, we will look inside the human mind for therein may reside the answer to the eternal question: “Is this computer, network, e-mail — and the list goes on — safe?”

Playing the Confidence Game

Running a con, or confidence game, is fairly straightforward: gain the trust of your targets and persuade them to want to give you something you want, like money or information. There are two basic ways con artists put people in a giving mood: self-interest and reciprocity.

Self-interest can be illustrated by a classic con known as the *Pigeon Drop*. Here is an example of how it works. Our “pigeon” is a bartender. On a slow night a guy comes out of the men’s room with a small black box and tells the bartender that he just found it in the men’s room. Inside the box is an expensive-looking ring. Just then the bar’s phone rings. On the other end of the line is a distraught gentleman asking if anyone found the ring he

bought for his wife for their wedding anniversary and offering a \$200 reward for its return. After hearing a description of the ring, the bartender tells him that a customer found it. The guy says, “Great, I’ll be there in half an hour!” and hangs up.

Now the fun begins. When the bartender tells the “customer” about the reward, the guy holding the ring says he can’t wait because he is in a hurry. He then offers to split the reward: *If the bartender will give him \$100, he will leave the ring with the bartender.* At this point, if the bartender has been taken in by the scam, he hands over \$100 and waits for the guy with the reward.

Unfortunately, 99 times out of 100, the ring, or cell phone, or purse, or necklace, is a fake. The only people splitting any money are the two guys with the bartender’s \$100.

Now, if we have the most advanced thinking devices on the planet, why does a con like this work? There are two factors at work here. The first, and most obvious, is simple greed. Free money? Great! Count me in!

The second factor, though, requires some understanding of neuroscience, specifically, a phenomenon called *The Human Oxytocin Mediated Attachment System*. THOMAS is, according to Dr. Paul Zak, author of The Moral Molecule blog, “a powerful brain circuit that releases the neurochemical oxytocin when we are trusted and induces a desire to reciprocate the trust we have been shown — even to strangers.”

This reaction helps form the basis for a successful con. By appearing vulnerable, and even respectable, a con can trigger a response in us to be helpful. It is not that we trust the con, but that *we think he trusts us*. Con artists take advantage of the same biochemical reaction that is the basis of our attachments to friends and family and a reward for cooperative actions of all kinds.

So, aside from the desire for the reward money, THOMAS rewards us with a feel-good shot of oxytocin for wanting to help the poor guy who lost his wife’s anniversary present. THOMAS is apparently very easy to stimulate in most people.

Our defense against this effect is our prefrontal cortex, the deliberative, decision-making region of our brain. Here is where we need to listen to that little voice of reason that says: *This is too good to be true.*

So how do we stimulate the prefrontal cortex? Any activity that engages logic or memory appears to help, like memorizing phone numbers or mentally calculating the tip on a restaurant bill. Perhaps we are, as a species, becoming more susceptible to being fooled because we do less of this type of thinking and off-load these tasks to our personal digital assistants or calculators.

Do A Good Deed Daily

Taking advantage of THOMAS is not the only way to work a con. Let’s look at a few examples of social engineering offered by uber-hacker Kevin Mitnick, in his book, *The Art of Deception*.

✓ To gain access to a computer system protected by a daily password change, wait for a snowstorm and call the network center posing as a snowed-in employee who wants to work from home and convince the operator to reveal the current password.

This one is less a trust issue than one of empathy or pity. To pull this off, the hacker must know the name of one or more employees and be capable of pulling off a convincing impersonation of a company employee. Those of us who live near the

Canadian border do tend to be pretty sympathetic to our friends and neighbors during blizzards.

✓ Gain proprietary information about a start-up company, then wait until the chief executive officer is out of town and show up at the company pretending to be a close friend of the CEO. Again, not a ploy that really takes advantage of the THOMAS phenomenon, but a common con all the same, particularly in any organization with a lot of new employees who do not know each other or their new boss well.

Here, the con man wants to give the impression that he will put in a good word for the helpful employee (*who has actually helped him infiltrate the company*) with the new boss.

✓ To gain access to a restricted area, approach the door carrying a large heavy-looking box and rely on a Good Samaritan to hold the door open for you. This one probably stimulates the THOMAS phenomenon because the target is helping a poor unfortunate staggering under the weight of a mighty load. Try this during a blizzard or other nasty weather to increase your chances for entry.

Let's face it, we are social creatures wired to help each other. Cooperative effort is how humans rose to the top of the food chain. Except for a very small percentage of the population who apparently lack THOMAS, which Dr. Zak estimates to be 2 percent, humans thrive on helping each other. The problem is that the other 2 percent are more than happy to take advantage of our helpful nature.

Chain Reactions

Isolated, single examples of social engineering may seem of limited harm. But good social hackers do not go for a big score all at once. They use a series of small exploits to score a big win.

Hackers approach social engineering through a psychological method. They attempt to create a perfect attack environment through impersonation, intimidation, ingratiation, conformity, diffusion of responsibility and friendliness. Their objective is to convince the person disclosing the information that they can be *trusted* with sensitive information.

The other important ingredient to their success is not to ask for too much information at one time so people do not become suspicious and are thus duped into providing valuable information bit by bit. By chaining related cons together, hackers can link these seemingly inconsequential pieces of information to gain access to an organization's systems — without launching a single piece of attack software.

Who Am I?

Social hackers often solicit information through impersonation. Impersonations generally fall into two categories: someone with a support job allegedly trying to provide help or someone with or close to authority. Common roles include: repairmen, IT techs, managers, trusted third parties (e.g., an executive assistant to a VIP), or fellow employees. The simple version of this attack is to call people pretending to be an employee and see what they will tell you. Here are some examples that have allegedly worked.



✓ A hacker calls unsuspecting targets and claims that he is from their telecommunications company's security division. He asks if a two-hour phone call has just been made to Israel. When the target vehemently denies this, the hacker says that he can remove the charges, but needs the target's calling card and PIN number. The target gratefully provides the information.

✓ A hacker calls the help desk and asks to be passed on to a supervisor. Once connected, the hacker expresses sympathy for the supervisor, who asks why. The hacker says that he is a system administrator and that from his console he can tell that systems are down. When the supervisor expresses surprise, he tells her to log in and out several times, each time claiming that he

cannot see any activity at his end. Eventually, he tells her that the only way he will be able to isolate the problem is if she gives him her account login information. Since she believes, at least at this point, that he is legitimate, she does.

Here is a more complex exploit that has apparently been replicated more than once by security testers.

✓ The hacker starts by sending an e-mail to a target organization, that we will refer to here as "Acme Widgets," asking about upcoming jobs. With any luck the reply will contain Acme's e-mail signature, its title and address formats, and whatever e-mail confidentiality statement is included in its official message.

Then the hacker registers a domain similar to the company's domain name. If the actual domain is "acmewidgets.com," the hacker might try "acmewjdgets.com." The hacker then creates a mail server with the fake domain and sends an e-mail to Acme employees from an account named "Help Desk" with a compressed file attachment that contains a keyboard logger. If this spyware is unique, it will not likely be included in standard antivirus profiles and may not be discovered by most antivirus or anti-spyware software.

The bogus e-mail instructs employees to run the attached file as part of an antivirus upgrade. Since the message may look legitimate to some of the targeted employees, they will follow the instructions and install the hacker's spyware, which subsequently sends an e-mail, with possibly sensitive data, at the end of each day back to the hacker.

Who Are They?

Another common social engineering attack method is to obtain a complete list of an organization's IT personnel and their contact information. The goal is to determine the usernames of the people likely to have the greatest access to an organization's networks.

This hack takes the form of a phone call to the fictional Acme Widget's human resources department. The hacker says that he was there earlier in the week for a job interview and wants to send thank-you notes to the people who interviewed him, for example, the chief information officer, IT director and two network administrators. However, curse his bad memory, he cannot remember their names and has lost or misplaced their business cards.

In telling the HR person how embarrassed he is about this, he attempts to trigger THOMAS and get names and as much other information as he can — whatever he can con out of the sympa-

thetic person on the other end of the phone. If this attempt is successful, the hacker can now move on to trying to collect other information. He will probe various offices to find out how willing people are to share information. The next couple of questions could look something like this ...

I have a meeting tomorrow with your IT engineering manager, Chad Thomas. Where is he located, please?

I am out of my office at the moment. What is our help desk number, please?

If he's been successful in all the previous intelligence gathering methods, our hacker now has enough information to try a more elaborate impersonation, particularly if he has established a relationship with some employees during earlier calls ...

Hi! My name is Ron. I'm a co-op, and I work with Chad Thomas and Pete Harmon in the network engineering office on the third floor in our Taft Corners office in Williston. They told me to give you a call because we are making some changes to the network, and I need to get some information from you.

At this point, the hacker can try to solicit more detailed information by "helping" employees report the IP address of their computer, or even tricking IT personnel into sending a complete organizational list of employees and account names.

All these social hacks, by themselves, may seem relatively harmless or even improbable. However, security personnel will tell you that not only can they work, they have worked, and are likely occurring somewhere as you read this.

As a result, hackers get lists of employees, administrator user IDs, data from keyboard loggers, useful jargon and other unique data that they can use to pass themselves off as authentic employees. Once hackers establish a certain level of credibility, they go after the real prizes: passwords, root level access to systems, and financial or operational data.

User, Know Thyself

Virtually every organization, public or private, in the United States requires annual computer security training for employees. But much of the focus is on preventing potential threats to the computer and on the network — turn off macros, do not download strange files and lock down system configurations — all good advice.

But our overall approach should be education in all security disciplines — physical, operational, informational and technological, and should include a strong coordinated approach to recognizing and responding to social hacking as a universal threat not limited to one area of security.

Educating people to defend themselves against social engineering is not a new concept. I remember watching a film in Air Force Basic Training in 1981 warning about these types of tactics in the context of the Cold War.

In the training film, spies asked seemingly innocent questions

about people and places at a base and gathered enough information to waylay a courier and steal the classified documents he was carrying.

If we are serious about defending ourselves against social engineering attacks, we need to educate users. In particular, we need to impress on personnel that they are the gatekeepers for organizational information and help them spot and report potential scams.

Our gatekeepers are secretaries, administrative employees, human resources employees, help desk technicians and other people in our organizations who answer the phones or respond to inquiries from the public.

Do we want them to be friendly and helpful? Of course, we do. But because they may be less sophisticated about security threats, they are the favorite targets of thieves and hackers.

We must teach employees how to identify the information they should protect and how to protect it. We must also teach employees how to recognize social engineering.

The Computer Security Institute provides tips to users that should trigger alarm when you are asked to provide information to unknown persons or from unsolicited e-mails. *If the caller or e-mailer ...*

- ✓ *Refuses to provide contact information*
 - ✓ *Exhibits undue haste for a response*
 - ✓ *Name-drops VIPs within the organization*
 - ✓ *Attempts to intimidate or ingratiate*
 - ✓ *Makes mistakes such as misspellings or misnomers*
 - ✓ *Asks odd questions or requests information that is for official use only*
- alert your security staff at once!*

The United States Computer Emergency Readiness Team, at www.us-cert.gov, offers training and guidance in spotting social engineering tactics and other computer security information.

We should establish and publicize procedures for reporting social engineering incidents to educate employees so they can avoid becoming targets too. I also suggest that some discussion of THOMAS should be part of every security training program. Maybe if people know how pleasure-inducing oxytocin rewards them for being helpful, they will be less likely to fall victim to hacker schemes.

Spies, con men and salesmen have been taking advantage of this mechanism for years, but it was only about four years ago that Zak demonstrated that this phenomenon exists and how it can be manipulated to scam innocent victims. Finally, we must recognize our social vulnerabilities and work to improve our behaviors, take time to think and use common sense. Don't let yourself or your network become a victim.

Until next time, Happy (Safe) Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a master of science degree in information resources management from the Air Force Institute of Technology. He currently serves as a telecommunications manager in the Department of Homeland Security. **CHIPS**

